WHAT IS INTERNET FRAUD?

Unwary investors are in danger today of being taken for a ride on the information superhighway. An estimated 4 million U.S. households that have access to the major online services are being exposed to hundreds of fraudulent and abusive investment schemes — including stock manipulations, pyramid scams and Ponzi schemes.

Many con artists today are technologically savvy. Swindlers are using the Internet to pull off their high-tech schemes in increasing numbers. Technology makes it easier for con artists to reach millions of people while masking their identities through false names and misinformation. Whether in the form of investments, work-at-home opportunities, Nigerian "officials," or new business ventures, almost anyone with an e-mail account has been exposed to shady solicitations.

The ever-increasing use of spam and pop-up windows gives con artists the chance to make offers to millions of people on any given day. Now, anytime an individual is logged on, he or she is likely to be solicited by unwanted offers for everything from personal ads to business opportunities. Technology advancement on the Internet is moving far too quickly for privacy filters to keep up. The growing number of spam e-mails and pop-ups continues to increase the necessity for people to arm themselves with information. Education is the only true way to avoid becoming a scam victim.

EXAMPLES OF INTERNET FRAUD

In May 2003, the U.S. Department of Justice busted one of the largest Internet investment fraud cases in the country. Alyn Waage (Canada) and Michael Webb (California) pleaded guilty to charges relating to the Tri-West Investment Club, an Internet-based investment scheme that brought in an estimated $60 million from its unsuspecting victims.

The con men developed a Web site that offered investments in prime bank notes, promising rates of return up to 120 percent, plus additional returns on any referrals. Not only did the club make promises of high return, but it also claimed to "guarantee" the investments. An informed investor should understand that extreme rates of return, guarantees on investments, and a focus on referrals are all major warnings of a fraudulent investment.

In addition to these red flags, the investment company was not registered with state or federal officials, as the law required. The investors' money was never invested in prime bank notes, but rather was used to pay off some of the earlier investors. Waage and Webb spent a vast majority of the money on an extravagant lifestyle, which was pulled from beneath them once they were brought to justice.

There are hundreds of other types of scams solicited via the Internet that are just as dangerous, including the following:

Nigerian 4-1-9 Scams
"Pump-and-Dump" Investment E-mails
Ponzi Schemes
Pyramid Schemes
International Lotteries
Work-at-Home Schemes

For specific information on any of these schemes, please contact the Investor Education Coordinator in Secretary of State Todd Rokita's office at **317.232.0734**.

The Honorable Todd Rokita
Indiana Secretary of State

The Office of the Indiana Secretary of State
Securities Division

O. Wayne Davis
Securities Commissioner

Stephanie L. Beck
Investor Education Coordinator

Kellie M. Duke
Director of Investor Education

To request additional copies of this or other materials, please contact:

Indiana Secretary of State Todd Rokita
Investor Education Program
302 West Washington Street
Room E-111
Indianapolis, Indiana 46204
Phone: 317.232.6681
Toll-free: 800.223.8791
Fax: 317.233.3675
www.IndianaInvestmentWatch.com

INDIANA INVESTMENT WATCH

Internet Fraud

www.IndianaInvestmentWatch.com

TEN TIPS FOR ONLINE INVESTORS

When you invest online, be sure to:

1. Obtain full disclosure, prior to opening your account, about the alternatives for buying and selling securities and how to obtain account information if you cannot access the firm's Web site.

2. Understand that most likely you are not linked directly to the market and that the click of your mouse does not instantly execute the trade.

3. Receive information from the firm to substantiate any advertised claims concerning the ease and speed of online trading.

4. Receive information from the firm about significant Web site outages, delays, and other interruptions to securities trading and account access.

5. Obtain information before trading about entering and canceling orders (market, limit, and stop loss) and the details and risks of margin accounts (borrowing to buy stocks).

6. Determine whether you are receiving delayed or real-time stock quotes and when your account information was last updated.

7. Review the firm's privacy and Web site security policies and whether your name may be used for mailing lists or other promotional activities by the firm or any other party.

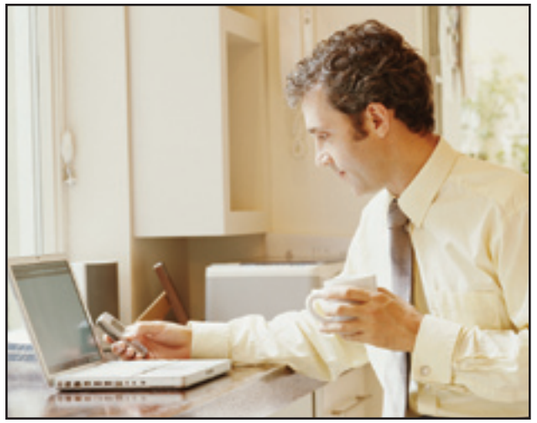
8. Receive clear information about sales commissions and fees and conditions that apply to any advertised discount on commissions.

9. Contact a customer service representative with your concerns, and don't hesitate to request prompt attention and fair consideration.

10. Contact Secretary of State Todd Rokita's office to (1) verify the registration/licensing status and disciplinary history of the online brokerage firm, or (2) file a complaint, if appropriate.

PHISHING SCAMS

Warnings are sounding, telling Americans everywhere to be watchful of a new, sophisticated form of Internet fraud. Various e-mail hoaxes are convincing consumers to visit falsified Web sites to update personal account information. This hoax, known as "phishing" in the technical world, is initiated by an e-mail stating an individual's brokerage, bank, or other account must be accessed immediately for various reasons. Some e-mails claim the individual's account has been mishandled, while others simply state the account information must be updated. The e-mails usually look very legitimate — using bank, brokerage, or company logos and official-sounding text. The individual is instructed to follow a link found within the e-mail to properly update and secure his/her account information. Unfortunately, the links in these e-mails redirect the user to non-secure sites not owned or operated by the financial institution, securities firm, or company mentioned in the e-mail; instead the link directs the user to a site operated by an Internet scammer. Once an individual follows the link within the e-mail, he/she runs the risk of giving the scam artist access to confidential personal information. The best way to avoid becoming a victim of a phishing scam is to delete the e-mail. The next time you log onto your account, the legitimate Web site will prompt you for updates if they are necessary.



HOW CAN INTERNET FRAUD BE AVOIDED?

Secretary Rokita's office would like to encourage investors to view the full version of NASAA's ***Internet Fraud and Abuse*** publication. This can be found by visiting NASAA's website at **www.nasaa.org**. The brochure is located in the **Investor Education** portion of the Web site under the link titled ***Investor Alerts and Tips.***

Another valuable resource is **www.investingonline.org**. This Web site offers unbiased, non-commercial facts about investing online and also has an interactive trading simulator.

SECRETARY OF STATE TODD ROKITA'S EFFORTS

As scams go high-tech, so have the efforts in Indiana Secretary of State Todd Rokita's office. The office is constantly making efforts to increase our electronic availability. Investment opportunities and securities agents may be checked via our Web site at **www.IndianaInvestmentWatch.com.** Many other investor education resources are also available on our Web site, and updates are available via e-mail. Additionally, complaint forms are available online and may be submitted electronically.

OTHER RESOURCES

For hard copies of the information listed below, please contact Indiana Secretary of State Todd Rokita's Investor Education Coordinator at **317.232.0734**.

The Federal Trade Commission has information concerning Internet fraud. Information about these can be obtained via the Web at **www.ftc.gov** — under the **For Consumers** section, click on **E-commerce & the Internet**.

Internet Auctions
Internet Access Services
Credit Card Fraud
International Modem Dialing
Web Cramming
International Lottery Scams
Chain Letters
Medical Billing Opportunities
Multilevel Marketing Plans/Pyramids
Travel and Vacation
Business Opportunities
Investments
Health Care Products/Services

The U.S. Department of Justice has information regarding the following schemes. This information can be obtained via the web at **www.internetfraud.usdoj.gov.**

Auction and Retail Schemes Online
Business Opportunities/Work-at-Home Schemes
Identity Theft and Fraud
Market Manipulation Schemes
Credit Card Schemes